



TITLE:

グレブナー基底算法における項キャンセルの一般論 (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

佐々木, 建昭

CITATION:

佐々木, 建昭. グレブナー基底算法における項キャンセルの一般論 (Computer Algebra : Design of Algorithms, Implementations and Applications). 数理解析研究所講究録 2012, 1815: 46-57

ISSUE DATE:

2012-10

URL:

<http://hdl.handle.net/2433/194572>

RIGHT:

グレブナー基底算法における項キャンセルの一般論

佐々木 建昭 (Tateaki Sasaki) *

筑波大学 名誉教授 (数学系)

PROFESSOR EMERITUS, UNIVERSITY OF TSUKUBA

Abstract

Buchberger の算法は浮動小数係数のグレブナー基底計算では非常に不安定であるが、その最大の理由は頻繁な項キャンセルによる巨大な桁落ち誤差の発生である。従来は Sylvester の恒等式に基づいて、ごく限られた場合にだけ正確な項キャンセルが証明されていた。本稿は、Buchberger 算法に現れる多項式を部分終結式もどきの行列式で表すことにより、組織的で正確な項キャンセルの一般論の構築する。

1 はじめに

本稿では、係数に誤差を含む多変数多項式系に対して、Buchberger 算法でグレブナー基底を計算することを念頭におく。この計算は非常に不安定であるが、その最大の理由は“正確で組織的な項キャンセル”によることが知られている。たとえば、次の簡単な入力に対して下記の連続した S 多項式計算を実行してみよう。

$$\begin{aligned} P_1 &= x^4y + x^2y - 2xy^2, & P_2 &= x^2y^3 + 2x^2y - 3xy^2 \\ P_3 &= \boxed{s}x^3y^2 + x^2y^2 - x^2y + 2xy^2 & /* \boxed{s} \text{は微小な数を表す} \\ P_4 &= \text{Spol}(P_1, P_3) = \boxed{s}yP_1 - xP_3 = -x^3y^2 + x^3y + (\boxed{s} - 2)x^2y^2 - 2\boxed{s}xy^3 \\ P_5 &= \text{Spol}(P_2, P_3) = \boxed{s}xP_2 - yP_3 = -x^2y^3 + 2\boxed{s}x^3y - (3\boxed{s} - 1)x^2y^2 - 2xy^3 \\ P_6 &= \text{Spol}(P_4, P_5) = yP_4 - xP_5 = \boxed{s} \times (-2x^4y + 3x^3y^2 + x^2y^3 - 2xy^4) \end{aligned}$$

P_6 の計算では、 \boxed{s} を含まない項が全て正確にキャンセルしている。この例は、正確な項キャンセルが組織的に起きることを示唆するとともに、 \boxed{s} が微小数のとき、キャンセル後には微小な項だけが残る、すなわち巨大な桁落ち誤差が生じることを示している。

上記の型の項キャンセルは論文 [10] で理論的に解明されており (2 章を参照)、もう少し別の場合も論文 [11] で扱われている。一般論は多項式剰余列の場合の部分終結式理論に対応し、算法で現れる多項式を入力多項式の係数ベクトルの行列式で表すことが目的である。一般論の構築は、1980 年代、Buchberger 自身や Collins らにより試みられ (論文 [6] 参照)、最終的に Mandache [6] により“部分終結式のような行列式表現は存在しない”と

*sasaki@math.tsukuba.ac.jp

されている。本稿は、部分終結式をかなり拡張すれば行列式表現が得られることを示す。ここで“拡張”とは、部分終結式の元となる行列からある列を除去したり、元となる行列にはない列や稀には行を付加することもある。行列式表現に基づけば、どのような場合にどの程度の大きさの項キャンセルが生じるかの解明は容易である。

2 従来研究のサーベイ

本章では種々の記号の定義をするとともに、上記の例を説明する理論を簡単に述べる。そして、部分終結式の拡張の一つとして、列の除去が頻繁に必要であることを示す。

変数 x, y, \dots, z の多項式を F や G 等と表し、それらの係数をそれぞれ f_i や g_j 等と表す。 \succ は多項式環 $\mathbb{C}[x, y, \dots, z]$ に設定された項順序とし、 \succ に関する F の最高順位項を主項といい $\text{lt}(F)$ と表し、その係数を主係数といって $\text{lc}(F)$ と表す。変数のべきの積をべき積という。 F の主項に現れるべき積を主べき積といい $\text{lpp}(F)$ と表す： $\text{lt}(F) = \text{lc}(F)\text{lpp}(F)$ 。 F と G の **S 多項式** を $\text{Spol}(F, G)$ と、 F の G による主項簡約を $\text{Lred}(F, G)$ と表す。後者は $F \xrightarrow{G}$ と図示することもある。 $F \xrightarrow{G} \tilde{F}$ は \tilde{F} が G 既約になるまでの連続簡約を意味する。

部分終結式を構成する際には、行列要素が多項式の係数となるように、多項式の割り算を擬除算で定義する。同様に、本稿の場合には **S 多項式** と主項簡約を次式で定義する。

$$\begin{aligned}\text{Spol}(F, G) &= \text{lc}(G) [L/\text{lpp}(F)] F - \text{lc}(F) [L/\text{lpp}(G)] G, \\ \text{Lred}(F, G) &= \text{lc}(G)F - \text{lc}(F) [\text{lpp}(F)/\text{lpp}(G)] G.\end{aligned}\tag{2.1}$$

ここで、 $L = \text{lcm}(\text{lpp}(F), \text{lpp}(G))$ である。 F と G が次式で与えられる場合をみよう。

$$F = f_1T_1 + f_2T_2 + \dots + f_mT_m, \quad G = g_1S_1 + g_2S_2 + \dots + g_nS_n \tag{2.2}$$

ただし T_i, S_j はべき積で、 $T_1 \succ T_2 \succ \dots \succ T_m$, $S_1 \succ S_2 \succ \dots \succ S_n$ とする。簡単のため、 $S_i = T_i$ ($i = 1, 2, \dots$) であるとすれば、 $\text{Spol}(F, G)$ は次式のように行列式で表現できる。

$$\begin{aligned}& g_1(f_1T_1 + f_2T_2 + \dots) - f_1(g_1T_1 + g_2T_2 + \dots) \\ &= \begin{vmatrix} g_1 & g_2 \\ f_1 & f_2 \end{vmatrix} T_2 + \begin{vmatrix} g_1 & g_3 \\ f_1 & f_3 \end{vmatrix} T_3 + \begin{vmatrix} g_1 & g_4 \\ f_1 & f_4 \end{vmatrix} T_4 + \dots\end{aligned}$$

上記のような行列式表現を行列で簡潔に表そう [2]。 M は $(k+1) \times n$ 行列, $n \geq k+1$, とし、第 i 列にはべき積 T_i を対応させる。 M の左 k 列と第 i 列, $i \geq k+1$, からなる行列式を c_i とすれば、行列 M と多項式 $P = \sum_{i=k+1}^n c_i T_i$ が一対一に対応する。このとき、 M を P に対する**簡約行列**という。例えば上記 $\text{Spol}(F, G)$ に対応する簡約行列は次である。

$$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & \dots \\ f_1 & f_2 & f_3 & f_4 & \dots \end{pmatrix} \tag{2.3}$$

$S_i = T_i$ が成立しない場合には条件が成立するように 0 係数項を付加する。 $S_1 = T_1$ さえ成立しない場合には、適当なべき積 S と T により $SS_i = TT_i$, ($i = 1, 2, \dots$), が成立するように 0 係数項を付加すればよい。一方、主項簡約の方は少し注意を要する。

より一般の $F \xrightarrow{G_1} F_1 \xrightarrow{G_2} \dots \xrightarrow{G_k} \tilde{F}$ なる簡約で説明する。ここで $G_i = G_j$ でもよい。このとき、 \tilde{F} は F, G_1, \dots, G_k とべき積 U_1, \dots, U_k により次のように表される。

$$\begin{cases} \tilde{F} = aF + b_1U_1G_1 + b_2U_2G_2 + \dots + b_kU_kG_k, \\ a = \prod_{i=1}^k \text{lc}(G_i), \quad b_1, b_2, \dots, b_k \in \mathbb{C}, \\ U_1G_1 \succ U_2G_2 \succ \dots \succ U_kG_k. \end{cases} \quad (2.4)$$

$\text{lc}(G_i) = g_{i,1}$, ($i = 1, \dots, k$), とおき、 F と U_1G_1, \dots, U_kG_k を次のように表す。

$$\begin{cases} F = f_1T_1 + f_2T_2 + \dots + f_nT_n + 0T_{n+1} + \dots, \\ U_1G_1 = g_{1,1}T_1 + g_{1,2}T_2 + \dots + \dots, \\ \vdots \\ U_kG_k = 0T_1 + \dots + g_{k,1}T_{k'} + g_{k,2}T_{k'+1} + \dots. \end{cases} \quad (2.5)$$

ここで $f_1, g_{1,1}, \dots, g_{k,1}$ は 0 ではないが、簡約行列の列を揃えるために、他の係数には 0 もあり得る (ほとんどの場合に、ある)。以下では、 $(f_1, f_2, \dots, f_n, 0, \dots)$, $(0, \dots, g_{i,1}, g_{i,2}, \dots)$ をそれぞれ F と U_iG_i の係数ベクトルと呼ぶ。 F, U_1G_1, \dots, U_kG_k の係数ベクトルを行とする行列がそのまま簡約行列にはならない場合があることを、例でみよう。

例 1 $F = x^2y - xy^2 + 2xy - 3y^2 + 2x$, $G = xy - y^2 - y$, \succ は全次数順序とする。 F は G で 2 回簡約され、 $F - xG - 3G = \tilde{F}$ となる。 F, xG, G に現れるべき積の集合は $\{x^2y, xy^2, xy, y^2, x, y\}$ であり、この集合上での F, xG, G の係数ベクトルからなる行列は

$$\left(\begin{array}{c|cccccc} & x^2y & xy^2 & xy & y^2 & x & y \\ \hline xG & 1 & -1 & -1 & 0 & & \\ G & & & 1 & -1 & 0 & -1 \\ F & 1 & -1 & 2 & -3 & 2 & 0 \end{array} \right)$$

となる。この行列の先頭の 2 列とそれぞれ第 3 列, ..., 第 6 列からなる四つの 3 次行列式はいずれも 0 になる。第 2 列を除去し、第 1 列と第 3 列およびそれぞれ第 4 ~ 第 6 列からなる三つの行列式を計算すれば、 $\tilde{F} = 0y^2 + 2x + 3y$ の各係数が得られる。◇

(2.5) の F, G_1, \dots, G_k に戻る。上記の例で第 2 列を除去する理由は、 $F \xrightarrow{G_1} F_1, F_1 \xrightarrow{G_2} F_2, \dots$ を表す行列式表現を順に構成していけば簡単に分かり、次の定理が得られる。

定理 1 ([10]) $F, G_1, \dots, G_k, \tilde{F}$ を上のように定めるとき、 \tilde{F} は次のように表現できる。

$$\tilde{F} = \sum_{i=1}^{n'-k} \begin{vmatrix} g_{1,1} & g_{1,2} & \dots & g_{1,k} & g_{1,k+i} \\ & g_{2,1} & \dots & g_{2,k-1} & g_{2,k-1+i} \\ & & \ddots & \vdots & \vdots \\ & & & g_{k,1} & g_{k,1+i} \\ f_1 & f_2 & \dots & f_k & f_{k+i} \end{vmatrix} T_{k+i} = \begin{vmatrix} g_{1,1} & g_{1,2} & \dots & g_{1,k} & U_1G_1 \\ & g_{2,1} & \dots & g_{2,k-1} & U_2G_2 \\ & & \ddots & \vdots & \vdots \\ & & & g_{k,1} & U_kG_k \\ f_1 & f_2 & \dots & f_k & F \end{vmatrix} \quad (2.6)$$

ここで簡約行列は、要素 $g_{1,1}, \dots, g_{k,1}$ が対角上にくるように、列が既に除去されており、べき積 $T_1, T_2, \dots, T_k, \dots$ は除去されずに残った列に順に対応するものとする。◇

定理 1 を使えば、第 1 章に例示した項キャンセルが次のように定式化される。多項式 F と F' が次式で与えられたとして、 $F \xrightarrow{G_1} \dots \xrightarrow{G_k} \tilde{F}$ と $F' \xrightarrow{G_1} \dots \xrightarrow{G_k} \tilde{F}'$ を考える。

$$\begin{aligned} F &= f_1 T_1 + f_2 T_2 + \dots + f_n T_n, & T_i &= T' T'_i \quad (i = 1, 2, \dots, n). \\ F' &= f'_1 T'_1 + f'_2 T'_2 + \dots + f'_n T'_n, \end{aligned} \quad (2.7)$$

定理 1 によれば、 \tilde{F} と \tilde{F}' は行列式で表現でき、 $\text{Spol}(\tilde{F}, \tilde{F}')$ の T_{k+i} 項の係数は

$$\begin{vmatrix} g_{1,1} & \cdots & g_{1,k} & g_{1,k+1} \\ & \ddots & \vdots & \vdots \\ & & g_{k,1} & g_{k,1+1} \\ f'_1 & \cdots & f'_k & f'_{k+1} \end{vmatrix} \cdot \begin{vmatrix} g_{1,1} & \cdots & g_{1,k} & g_{1,k+i} \\ & \ddots & \vdots & \vdots \\ & & g_{k,1} & g_{k,1+i} \\ f_1 & \cdots & f_k & f_{k+i} \end{vmatrix} - \begin{vmatrix} \text{same} \\ \vdots \\ \text{same} \\ f'_j \rightarrow f_j \end{vmatrix} \cdot \begin{vmatrix} \text{same} \\ \vdots \\ \text{same} \\ f_j \rightarrow f'_j \end{vmatrix} \quad (2.8)$$

$$= \begin{vmatrix} g_{1,1} & \cdots & g_{1,k} \\ & \ddots & \vdots \\ & & g_{k,1} \end{vmatrix} \cdot \begin{vmatrix} g_{1,1} & \cdots & g_{1,k} & g_{1,k+1} & g_{1,k+i} \\ & \ddots & \vdots & \vdots & \vdots \\ & & g_{k,1} & g_{k,1+1} & g_{k,1+i} \\ f'_1 & \cdots & f'_k & f'_{k+1} & f'_{k+i} \\ f_1 & \cdots & f_k & f_{k+1} & f_{k+i} \end{vmatrix} \quad (2.9)$$

と表現することができる。ここで、(2.8) から (2.9) への変換は Sylvester の恒等式による。この式によれば、 $\text{Spol}(\tilde{F}, \tilde{F}')$ の計算において、積 $g_{1,1} \cdots g_{k,1}$ を含まない項は全て正確にキャンセルすることがわかる。

上記の項キャンセルは、数値行列でピボットニングなしの場合のキャンセルと全く同じメカニズムによる。しかしながら、Buchberger 算法における項キャンセルは数値行列のキャンセルよりも複雑で、Sylvester の恒等式だけでは解明できない。

上記では非主項は簡約されていない。同様に、本稿を通じて次を仮定する。

前提 1 本稿では S 多項式生成と主項簡約だけを用いてグレブナー基底を計算する。得られる基底は未簡約基底であり、簡約基底が欲しい場合は最後に非主項を簡約する。

3 多項式剰余列型の簡約に対する行列式理論

部分終結式の定式化は Collins[2] らによりなされたが、かなり面倒である。Buchberger 算法における項簡約を部分終結式と同様に定式化すれば、はるかに面倒になるのは明白である。ところで、筆者と古川は [9] において多重多項式剰余列を定式化したが、そこでは“逆簡約”という方法が考案された。簡約手順を逆にたどりつつ簡約行列を構成する方法である。本章では、扱い易い多項式剰余列型の項簡約に対して逆簡約法で簡約行列を構成することにより、新しい定式化の簡潔さを示す。

次のような連続簡約を**多項式剰余列型の簡約**と呼ぶ。

$$P_1 \xrightarrow{P_2} P_3, P_2 \xrightarrow{P_3} P_4, \dots, P_{i-1} \xrightarrow{P_i} P_{i+1}, \dots \quad (3.1)$$

1 変数の場合、 (P_1, P_2, \dots, P_k) は多項式剰余列に他ならず、大きな項キャンセルが頻繁に起きることがよく知られている。多項式剰余列型の簡約に対しては部分終結式が素直に拡張できることを示す。(3.1)において、 $P_{i-1} \xrightarrow{P_i} P_{i+1}$ が P_{i-1} の P_i による k_i 回の簡約とするならば、 P_{i+1} は次のように表現できる。

$$P_{i+1} = \text{lc}(P_i)^{k_i} P_{i-1} + b_{i,1} U_{i,1} P_i + \dots + b_{i,k_i} U_{i,k_i} P_i \quad (3.2)$$

ここで、 $b_{i,1}, \dots, b_{i,k_i}$ は数であり、 $U_{i,1}, \dots, U_{i,k_i}$ はべき積で $U_{i,1} \succ \dots \succ U_{i,k_i}$ である。 $\text{supp}(P_{i-1}) \cup \bigcup_{j=1}^{k_i} \text{supp}(U_{i,j} P_i) = \{T_{i,1}, T_{i,2}, \dots, T_{i,n_i}\}$, $T_{i,1} \succ T_{i,2} \succ \dots \succ T_{i,n_i}$ とし、この集合上で係数ベクトルを定義すれば、 P_{i+1} は次の簡約行列で表現できる。

$$M_{i+1}^{(i)} = \begin{pmatrix} \text{coefficient vector of } U_{i,1} P_i \\ \ddots & \ddots & \ddots & \ddots \\ \text{coefficient vector of } U_{i,k_i} P_i \\ \text{coefficient vector of } P_{i-1} \end{pmatrix} \quad (3.3)$$

行列を P_{i-2} と P_{i-1} の係数ベクトルで表そう。(3.2)と同様、 P_i は次のように表せる。

$$P_i = \text{lc}(P_{i-1})^{k_{i-1}} P_{i-2} + b_{i-1,1} U_{i-1,1} P_{i-1} + \dots + b_{i-1,k_{i-1}} U_{i-1,k_{i-1}} P_{i-1} \quad (3.4)$$

まず、簡約行列に必要なべき積集合を $U_{i,1} P_{i-2}, \dots, U_{i,k_i} P_{i-2}, P_{i-1}, U_{i,1} U_{i-1,1} P_{i-1}, \dots, U_{i,1} U_{i-1,k_{i-1}} P_{i-1}, \dots, U_{i,k_i} U_{i-1,k_{i-1}} P_{i-1}$ に現れる全ての異なるべき積の集合に再定義する。次に、多項式 $U_{i,1} U_{i-1,1} P_{i-1}, \dots, U_{i,1} U_{i-1,k_{i-1}} P_{i-1}, \dots, U_{i,k_i} U_{i-1,k_{i-1}} P_{i-1}$ の係数ベクトルを行列 $M_{i+1}^{(i)}$ に付加して次の行列をつくる。

$$\tilde{M}_{i+1}^{(i)} = \begin{pmatrix} \text{coefficient vector of } U_{i,1} P_i \\ \ddots & \ddots & \ddots & \ddots \\ \text{coefficient vector of } U_{i,k_i} P_i \\ \text{coefficient vector of } U_{i,1} U_{i-1,1} P_{i-1} \\ \text{coefficient vector of } U_{i,1} U_{i-1,2} P_{i-1} \\ \ddots & \ddots & \ddots & \ddots \\ \text{coefficient vector of } U_{i,k_i} U_{i-1,k_{i-1}} P_{i-1} \\ \text{coefficient vector of } P_{i-1} \end{pmatrix} \quad (3.5)$$

前章に説明した理由で、主係数 $\text{lc}(P_{i-1})$ が $\tilde{M}_{i+1}^{(i)}$ の $(k_i + j, j)$ 要素, $(j = 1, 2, \dots)$, になるように、不必要な列は除去されるものとする。 $\text{lc}(P_{i-1})$ のべき乗を除けば、 $M_{i+1}^{(i)}$ と $\tilde{M}_{i+1}^{(i)}$ は同じ行列式表現を与える。(3.4)によれば、上記行列は $U_{i,j} P_{i-2}$, $(1 \leq j \leq k_i)$, を P_{i-1}

で簡約するのに十分な行を含む。したがって、 $\check{M}_{i+1}^{(i)}$ の上部 k_i 個の行を次式のように置き換えることができる。

$$M_{i+1}^{(i-1)} = \begin{pmatrix} \text{coefficient vector of } U_{i,1}P_{i-2} \\ \ddots & \ddots & \ddots & \ddots \\ \text{coefficient vector of } U_{i,k_i}P_{i-2} \\ \text{coefficient vector of } U_{i,1}U_{i-1,1}P_{i-1} \\ \text{coefficient vector of } U_{i,1}U_{i-1,2}P_{i-1} \\ \ddots & \ddots & \ddots & \ddots \\ \text{coefficient vector of } U_{i,k_i}U_{i-1,k_{i-1}}P_{i-1} \\ \text{coefficient vector of } P_{i-1} \end{pmatrix} \quad (3.6)$$

上記の手順を逆簡約と呼ぶが、これを繰り返すと次の定理が得られる。なお、以下では簡約行列 M が表す多項式を $\text{DetPol}(M)$ と表す。

定理 2 (3.1) で生成される各 P_i , ($3 \leq i \leq k$), は、 $\text{lc}(P_2), \dots, \text{lc}(P_{i-2})$ のべき乗倍を除けば、 P_1, P_2 とそのべき積倍の多項式の係数ベクトルからなる簡約行列で表現できる。◇

$M_{i+1}^{(i)}$ に付加される行の個数を $\#a$ とすれば、(3.3) と (3.5) より次式が得られる。

$$\text{DetPol}(M_{i+1}^{(i)}) = (-1)^{k_i \#a} \text{DetPol}(\check{M}_{i+1}^{(i)}) / \text{lc}(P_{i-1})^{\#a} \quad (3.7)$$

次に、行列 $\check{M}_{i+1}^{(i)}$ の P_i の係数ベクトルを P_{i-2} のそれで置き換えるためには、各ベクトルに $\text{lc}(P_{i-1})^{k_{i-1}}$ を掛ける必要がある。したがって、次式が成り立つ。

$$\text{DetPol}(\check{M}_{i+1}^{(i)}) = \text{lc}(P_{i-1})^{k_i k_{i-1}} \text{DetPol}(M_{i+1}^{(i-1)}) \quad (3.8)$$

これらより、次の命題が直ちに得られ、行列 $M_{i+1}^{(i)}$ と $M_{i+1}^{(i-1)}$ の各要素が関連する多項式の係数であることから、系も簡単に得られる (証明略)。

命題 1 上記の記号の下、次の関係式が成立する。

$$\text{DetPol}(M_{i+1}^{(i)}) = (-1)^{\#a k_i} \text{lc}(P_{i-1})^{k_i k_{i-1} - \#a} \text{DetPol}(M_{i+1}^{(i-1)}) \quad (3.9)$$

系 1 上記の記号の下、 $\#a < k_i k_{i-1}$ ならば、 $P_{i-1} \xrightarrow{P_i} P_{i+1}$ において、 $\text{lc}(P_{i-1})^{k_i k_{i-1} - \#a}$ を含まない項は正確にキャンセルする。さらに、 $|\text{lc}(P_{i-1})| \ll \|P_{i-1}\|$ ならば、キャンセルする項は主要項 (多項式の中で係数が相対的に大きい項) である。◇

4 S 多項式にかかわる簡約に対する行列式理論

第 2 章において、Buchberger 算法の典型的な項簡約に対する簡約行列の構成では列を除去する必要性が頻繁に生じることを示した。本章では、逆に列を追加する必要性も頻繁に生じることを示す。

まず、次のような S 多項式の簡約を考える。

$$S \stackrel{\text{def}}{=} \text{Spol}(F, G) \xrightarrow{H_1} \dots \xrightarrow{H_k} \tilde{S} \quad (4.1)$$

ここで、 H_1, H_2, \dots, H_k には同じものがあってもよい。 \tilde{S} はべき積 U_1, U_2, \dots, U_k で次のように表される。

$$\begin{cases} \tilde{S} = aS + b_1 U_1 H_1 + b_2 U_2 H_2 + \dots + b_k U_k H_k, \\ a = \prod_{i=1}^k \text{lc}(H_i), \quad b_1, b_2, \dots, b_k \in \mathbb{C}, \\ U_1 H_1 \succ U_2 H_2 \succ \dots \succ U_k H_k. \end{cases} \quad (4.2)$$

一般性を失うことなく、 $\text{lpp}(F) = \text{lpp}(G) = T_0$ を仮定する。 $\text{lc}(F) = f_0$ 、 $\text{lc}(G) = g_0$ 、 $\text{lc}(H_i) = h_{i,1}$ 、 $(i=1, \dots, k)$ 、とおき、 $\{T_0, T_1, T_2, \dots\} = \text{supp}(F) \cup \text{supp}(G) \cup \bigcup_{i=1}^k \text{supp}(H_i)$ 、 $T_0 \succ T_1 \succ T_2 \succ \dots$ 、とする。すると、 F や G などは次のように表される。

$$\begin{cases} F = f_0 T_0 + f_1 T_1 + \dots + f_m T_m + 0T_{m+1} + \dots, \\ G = g_0 T_0 + g_1 T_1 + \dots + g_n T_n + 0T_{n+1} + \dots, \\ U_1 H_1 = h_{1,1} T_1 + h_{1,2} T_2 + \dots + \dots, \\ \vdots \\ U_k H_k = 0T_1 + \dots + h_{k,1} T_{k'} + h_{k,2} T_{k'+1} + \dots. \end{cases} \quad (4.3)$$

ここで、係数 f_j, g_j ($j \geq 1$)、 $h_{i,j'}$ ($j' \geq 2$) の中には 0 があってもよい。次の定理は逆簡約の操作から簡単に証明できるので、証明は省略する。

定理 3 \pm 符号を除けば、 \tilde{S} は次の簡約行列で表すことができる。ただし、主係数 $h_{i,1}$ 、 $(i=1, \dots, k)$ 、が $(i+1, i)$ 要素になるよう、余分な列は除去されるものとする。

$$\begin{pmatrix} f_0 & f_1 & f_2 & f_3 & \dots & \dots \\ g_0 & g_1 & g_2 & g_3 & \dots & \dots \\ & h_{1,1} & h_{1,2} & h_{1,3} & \dots & \dots \\ & & \ddots & \ddots & \ddots & \dots \\ & & & h_{k,1} & h_{k,2} & \dots \end{pmatrix} \quad \diamond \quad (4.4)$$

次に、 S 多項式による簡約を考える。まず、例で説明する。

例 2 (S 多項式による項簡約)

$$H = 2x^2y^2 + 3x^2y + y^2 - 5, \quad F = 2x^2y^2 - x^2y + x^2, \quad G = 3x^2y^2 - 2x^2y + y^2$$

に対して、 $S \stackrel{\text{def}}{=} \text{Spol}(F, G) = x^2y + 3x^2 - 2y^2$ で H を簡約すると、次のようになる。

$$H \xrightarrow{S} \tilde{H}, \quad \tilde{H} = 4y^3 + 9x^2 - 5y^2 - 5$$

\tilde{H} の簡約行列は、 H, yS, S の係数ベクトルで次のように表すことができる。

$$\left(\begin{array}{c|cccccc} & x^2y^2 & x^2y & y^3 & x^2 & y^2 & 1 \\ \hline yS & 1 & 3 & -2 & & & \\ S & & 1 & & 3 & -2 & \\ H & 2 & 3 & & & 1 & -5 \end{array} \right)$$

$S = 3F - 2G$ なので、 S の係数ベクトルを F と G のそれで表し、次の行列を作る：行数と列数の増加量を等しくするため、べき積 x^2y^2 に対応する列を追加したことに注意。

$$\left(\begin{array}{c|cccccccc} & x^2y^2 & x^2y^3 & x^2y^2 & x^2y & y^3 & x^2 & y^2 & 1 \\ \hline yG & & 3 & -2 & & 1 & & & \\ yF & & 2 & -1 & 1 & & & & \\ G & 3 & & 3 & -2 & & & 1 & \\ F & 2 & & 2 & -1 & & 1 & & \\ H & & & 2 & 3 & & & 1 & -5 \end{array} \right) \quad (4.5)$$

第 1 列を消去してみれば、上記行列は \pm 符号を除き \tilde{H} を与えることが分る。 \diamond

例 2 は容易に複数の S 多項式 S_1, \dots, S_k による H の簡約に一般化できる：

$$H \xrightarrow{S_1} \dots \xrightarrow{S_k} \tilde{H} \quad (4.6)$$

ここで、 $S_i = \text{Spol}(F_i, G_i)$, ($i = 1, \dots, k$), である。各多項式を次のように表す。

$$\begin{cases} F_i = f_{i0}T_{i0} + f_{i0+1}T_{i0+1} + f_{i0+2}T_{i0+2} + \dots, & f_{i0} \neq 0, \\ G_i = g_{i0}T_{i0} + g_{i0+1}T_{i0+1} + g_{i0+2}T_{i0+2} + \dots, & f_{i0} \neq 0, \\ H = h_1T_1 + h_2T_2 + h_3T_3 + \dots, & h_1 \neq 0. \end{cases} \quad (4.7)$$

ここで、 $T_{i0} \succ T_{20} \succ \dots \succ T_{k0}$ かつ $T_{k0} \succ T_1 \succ T_2 \succ T_3 \succ \dots$ である。

定理 4 \pm 符号を除けば、 \tilde{H} は次の簡約行列で与えられる (証明略)。

$$\left(\begin{array}{c|c|cccccccc} & & & f_{1,0} & f_{1,1} & f_{1,2} & f_{1,3} & \cdots & \cdots & \cdots \\ & & & g_{1,0} & g_{1,1} & g_{1,2} & g_{1,3} & \cdots & \cdots & \cdots \\ f_{2,0} & & & & f_{2,0} & f_{2,1} & f_{2,2} & f_{2,3} & \cdots & \cdots \\ g_{2,0} & & & & g_{2,0} & g_{2,1} & g_{2,2} & g_{2,3} & \cdots & \cdots \\ & & & & & \ddots & \ddots & \ddots & \ddots & \cdots \\ & & & & & & f_{k,0} & f_{k,1} & f_{k,2} & \cdots \\ & & & & & & g_{k,0} & g_{k,1} & g_{k,2} & \cdots \\ & & & & & & h_1 & \cdots & h_k & h_{k+1} & h_{k+2} & \cdots \end{array} \right) \quad \diamond \quad (4.8)$$

5 Buchberger 算法における項キャンセルの一般論

本章では、多重多項式剰余列を少し拡張する形で Buchberger 算法を捉えることにより、多重多項式剰余列理論をベースに Buchberger 算法における項簡約を定式化する。ただし、多重多項式剰余列理論は複雑なので理論の詳細は省き、定理とその証明の概要を述べる。その定理に基づき、Buchberger 算法における項キャンセルの一般論を展開する。

定義 1 (多重多項式剰余列型の項簡約) 与えられた多項式集合を $\{F_1^{(0)}, F_2^{(0)}, \dots, F_s^{(0)}\}$, $s \geq 3$, とする。第 i 番目の集合 (初期集合でもよい) $\{F_1^{(i)}, F_2^{(i)}, \dots, F_s^{(i)}\}$ を計算したとすると、その中から一つの要素 $F_r^{(i)}$ を選んで他の要素を簡約し、第 $(i+1)$ 番目の集合 $\{F_1^{(i+1)}, F_2^{(i+1)}, \dots, F_s^{(i+1)}\}$ を次の算式で計算する。

$$F_j^{(i)} \xrightarrow{F_r^{(i)}} F_j^{(i+1)} \quad (\forall j \neq r), \quad F_r^{(i)} = F_r^{(i+1)} \quad (5.1)$$

当然、 $F_j^{(i)} = F_j^{(i+1)}$ のこともあり得る。最後の集合を $\{F_1^{(\lambda)}, F_2^{(\lambda)}, \dots, F_s^{(\lambda)}\}$ とする。◇

多重多項式剰余列型の項簡約に対しても、多項式剰余列型の項簡約と同様、簡約行列が簡単に構成できそうに思えるが、そうではない。非常に稀であるが、逆簡約の過程でごく一部の列にだけ非零要素を持つ行を付加する必要性が生じる。その説明が多重多項式剰余列理論の主要部分を成すが、その仕組みはかなり複雑である。したがって、詳細については論文 [9] を参照して頂くとして、本稿では紙面の制約もあり割愛する。

本稿では、Buchberger 算法を多重多項式剰余列を修正する形で次のように定式化する。 $S = \text{Spol}(F_{j_1}^{(i)}, F_{j_2}^{(i)})$ が生成された場合には、 S は集合 $\{F_1^{(i+1)}, \dots, F_{s'}^{(i+1)}\}$ に加える。 $F_j^{(i)}$ が 0 に簡約された場合には、 $F_j^{(i)}$ は集合から除去する。そして、最も重要なことであるが、別の多項式で簡約する度に、次の集合に移行するものとする。こうすれば、簡約行列の構成という点では多重多項式剰余列理論がそのまま使える。

定理 5 (主定理) Buchberger 算法に現れる任意の多項式に対して簡約行列を構成できる。簡約行列は、列に関してブロック構造をしており、その行は入力多項式とそのべき積倍の“拡張係数ベクトル”である。ここで、列ブロックとは行列 (4.8) でいえば縦線で囲まれた列集合であり、拡張係数ベクトルとは、一つの行は一つの多項式の係数のみを要素とし、各ブロック内では係数が高次から低次へと並べられて、さらに余分な列に対応する係数が除かれたものである。

証明 初期基底を $\{F_1^{(0)}, \dots, F_s^{(0)}\}$ 、中間基底を $\{F_1^{(i)}, \dots, F_{s'}^{(i)}\}$, $(i \geq 1)$ 、最終基底 (Gröbner 基底) を $\{F_1^{(\lambda)}, \dots, F_t^{(\lambda)}\}$ とする。実際は最終基底が Gröbner 基底であることを確認するためにも計算が必要で、上述の多重多項式剰余列との対応では、その計算でも基底番号が増加するが、その計算は上記定理には無関係なので無視する。

$i = \lambda - 1$ の場合: $F_l^{(\lambda)} = \text{Spol}(F_{j_1}^{(\lambda-1)}, F_{j_2}^{(\lambda-1)})$ ならば、 $F_l^{(\lambda)}$ は、 $F_{j_1}^{(\lambda-1)}$ と $F_{j_2}^{(\lambda-1)}$ の係数ベクトルを行とする (2.3) のような簡約行列で表される。 $F_l^{(\lambda-1)} \xrightarrow{F_r^{(\lambda-1)}} F_l^{(\lambda)}$ ならば、 $F_l^{(\lambda)}$ は (2.6) において $G_1 = \dots = G_k = F_r^{(\lambda-1)}$ とした式に対応する簡約行列で表される。

$i \leq \lambda - 2$ の場合: $F_l^{(\lambda)}$ が $F_1^{(i+1)}, \dots, F_{s''}^{(i+1)}$ 及びそれらのべき積倍の多項式の拡張係数ベクトルを行とする簡約行列 $M_l^{(i+1)}$ で表されると仮定する。証明すべきは行列 $M_l^{(i+1)}$ が $F_1^{(i)}, \dots, F_{s'}^{(i)}$ の係数を要素とする簡約行列 $M_l^{(i)}$ に変換できることである。

- $F_l^{(i+1)} = \text{Spol}(F_{j_1}^{(i)}, F_{j_2}^{(i)})$ の場合。 $F_l^{(i+1)}$ の拡張係数ベクトルを、行列 (4.4) のように、 $F_{j_1}^{(i)}$ と $F_{j_2}^{(i)}$ の拡張係数ベクトルで置き換えればよい。2 個以上の行ベクトルを置き換える場合は、行列 (4.8) のように新たな列ブロックを追加する。

- $F_l^{(i)} \xrightarrow{F_r^{(i)}} F_l^{(i+1)}$ で $F_r^{(i)}$ が S 多項式でない場合。第 3 章のように、 $F_r^{(i)}$ の係数ベクトルから成る行を必要なだけ $M_l^{(i+1)}$ に付加し、 $F_l^{(i+1)}$ の係数ベクトルを $F_l^{(i)}$ の係数ベクトルで置き換えればよい。

- $F_l^{(i)} \xrightarrow{F_r^{(i)}} F_l^{(i+1)}$ で $F_r^{(i)} = \text{Spol}(F_{j_1}^{(i)}, F_{j_2}^{(i)})$ の場合。 (4.8) が示すように、 $M_l^{(i)}$ における $F_r^{(i)}$ とそのべき積倍多項式の拡張係数ベクトルを $F_{j_1}^{(i)}$ と $F_{j_2}^{(i)}$ の拡張係数ベクトルで置き換え、必要なだけ新たな列ブロックを追加すればよい。 ◇

これまで述べた行列式理論によれば、項キャンセルのメカニズムは明快に理解できる。そのためには、S 多項式の生成と主項簡約のあらゆる組合せについて、具体的に行列式の振舞いを解析すればよい。本稿では典型的な二つの場合を記述するが、残る場合も同様に簡単に解析できることを指摘しておく。

【場合 I】 $F_1 \xrightarrow{G_{1,1}} \dots \xrightarrow{G_{1,r_1}} \tilde{F}_1, F_2 \xrightarrow{G_{2,1}} \dots \xrightarrow{G_{2,r_2}} \tilde{F}_2$ に対して、 $S = \text{Spol}(\tilde{F}_1, \tilde{F}_2)$ 。

各簡約を 1 回のみにしたことに注意されたい。当然、 $G_{i,j_1} = G_{i,j_2}$ であってもよい。これは定理 1 で扱った演算を一般化したものだが、Sylvester の恒等式では解析できない。

簡単のため、 F_1 と F_2 にはすでに必要なべき積が掛けられ、 $F_i = f_{i,1}T_1 + f_{i,2}T_2 + \dots$ かつ $\tilde{F}_i = \tilde{f}_{i,1}\tilde{T}_1 + \tilde{f}_{i,2}\tilde{T}_2 + \dots$, ($i = 1, 2$), であるとする。ここで、 $T_1 \succ T_2 \succ \dots$ かつ $\tilde{T}_1 \succ \tilde{T}_2 \succ \dots$ である。すると、 S は次の簡約行列 \tilde{M}_S で表される。

$$\tilde{M}_S = \begin{pmatrix} \tilde{f}_{2,1} & \tilde{f}_{2,2} & \tilde{f}_{2,3} & \cdots \\ \tilde{f}_{1,1} & \tilde{f}_{1,2} & \tilde{f}_{1,3} & \cdots \end{pmatrix} \quad (5.2)$$

$\tilde{F}_i = [\text{lc}(G_{i,1}) \cdots \text{lc}(G_{i,r_i})] F_i - c_{i,1}U_{i,1}G_{i,1} - \dots - c_{i,r_i}U_{i,r_i}G_{i,r_i}$, ($i = 1, 2$), とする。ここで、 $c_{i,1}, \dots, c_{i,r_i}$ は数で $U_{i,1}, \dots, U_{i,r_i}$ はべき積である。 $U_{1,j_1}G_{1,j_1}$ と $U_{2,j_2}G_{2,j_2}$ が定数倍を除き等しい場合は両者を同一視して、 $\{G'_1, G'_2, \dots, G'_s\} := \cup_{i=1}^2 \{U_{i,j}G_{i,j} \mid j=1, \dots, r_i\}$, $G'_1 \succ G'_2 \succ \dots \succ G'_s$ とする。行列 (3.3) から (3.5) への変換のように、上記行列 \tilde{M}_S に G'_1, G'_2, \dots, G'_s の係数ベクトルを付加し、 \tilde{F}_1 と \tilde{F}_2 の係数ベクトルをそれぞれ F_1 と F_2 の係数ベクトルで置き換える。すると、 \tilde{M}_S は次の簡約行列に変換される。

$$M_S = \begin{pmatrix} g'_{1,1} & g'_{1,2} & \cdots & \cdots & \cdots \\ & \ddots & \ddots & \cdots & \cdots \\ & & g'_{s,1} & g'_{s,2} & \cdots \\ f_{2,1} & \cdots & f_{2,s} & \cdots & \cdots \\ f_{1,1} & \cdots & f_{1,s} & \cdots & \cdots \end{pmatrix} \quad (5.3)$$

上記変換においては、 F_1 と F_2 にそれぞれ $\text{lc}(G_{1,1}) \cdots \text{lc}(G_{1,r_1})$ と $\text{lc}(G_{2,1}) \cdots \text{lc}(G_{2,r_2})$ を掛ける必要がある。したがって、次の関係式を得る。

$$\begin{aligned} \text{DetPol}(\tilde{M}_S) &= C \text{DetPol}(M_S), \quad \text{where} \\ C &= [\prod_{i=1}^2 \text{lc}(G_{i,1}) \cdots \text{lc}(G_{i,r_i})] / [\text{lc}(G'_1) \cdots \text{lc}(G'_s)] \end{aligned} \quad (5.4)$$

命題 2 $\tilde{F}_1, \tilde{F}_2, G_{1,j}, G_{2,j}, r_1, r_2, s, C$ 等は上で定義されたものとする。 $r_1 + r_2 > s$ ならば、 $S = \text{Spol}(\tilde{F}_1, \tilde{F}_2)$ の計算において、 $\text{lc}(G_{1,j})$ と $\text{lc}(G_{2,j})$, ($j=1, 2, \dots$), を独立なパラメータとみなすとき、 C を含まない全ての項は互いにキャンセルする。

証明 初めに、 $r_1 + r_2 > s$ なので、 C の分母は分子を割り切ることを指摘しておく。 $S = \text{DetPol}(\tilde{M}_S)$ であり $\text{DetPol}(M_S)$ 各要素は $F_1, F_2, G'_1, \dots, G'_s$ の係数なので、命題は (5.4) から直ちに得られる。◇

【場合 II】 $F \xrightarrow{H_{0,1}} \cdots \xrightarrow{H_{0,r_0}} \tilde{F}$, $G_i \xrightarrow{H_{i,1}} \cdots \xrightarrow{H_{i,r_i}} \tilde{G}_i$, ($i=1, \dots, q$), に対し、 $\tilde{F} \xrightarrow{\tilde{G}_1} \cdots \xrightarrow{\tilde{G}_q} R$ 。
 $R = \tilde{c}_0 \tilde{F} - \tilde{c}_1 \tilde{U}_1 \tilde{G}_1 - \cdots - \tilde{c}_q \tilde{U}_q \tilde{G}_q$ とする。ここで、 $\tilde{c}_0, \tilde{c}_1, \dots, \tilde{c}_q$ は数で $\tilde{U}_1, \dots, \tilde{U}_q$ はべき積である。 R は次の簡約行列で表される。

$$\tilde{M}_R = \begin{pmatrix} \text{coefficient vector of } \tilde{U}_1 \tilde{G}_1 \\ \ddots & \ddots & \ddots \\ \text{coefficient vector of } \tilde{U}_q \tilde{G}_q \\ \text{coefficient vector of } \tilde{F} \end{pmatrix} \quad (5.5)$$

$\tilde{F} = c_{0,0}F - \sum_{j=1}^{r_0} c_{0,j}U_{0,j}H_{0,j}$ および $\tilde{G}_i = c_{i,0}G_i - \sum_{j=1}^{r_i} c_{i,j}U_{i,j}H_{i,j}$, ($1 \leq i \leq q$), とする。ここで、 $c_{i,0}, \dots, c_{i,r_i}$ は数で $U_{i,1}, \dots, U_{i,r_i}$ はべき積である。場合 I と同様、 $\{H'_1, \dots, H'_s\} := \cup_{i=0}^q \{U_{i,j}H_{i,j} \mid j=1, \dots, r_i\}$, $\text{lpp}(H'_1) \succ \cdots \succ \text{lpp}(H'_s)$, とする。上記行列 \tilde{M}_R に H'_1, \dots, H'_s の係数ベクトルを付加し、 \tilde{F} と \tilde{G}_i の係数ベクトルをそれぞれ F と G_i の係数ベクトルで置き換えると、次の簡約行列 M_R を得る。

$$M_R = \begin{pmatrix} \text{coefficient vector of } H'_1 \\ \text{coefficient vector of } H'_2 \\ \ddots & \ddots & \ddots \\ \text{coefficient vector of } H'_s \\ \text{coefficient vector of } \tilde{U}_1 G_1 \\ \ddots & \ddots & \ddots \\ \text{coefficient vector of } \tilde{U}_q G_q \\ \text{coefficient vector of } F \end{pmatrix} \quad (5.6)$$

場合 I と同様、簡約行列 \tilde{M}_R と M_R の間には次の関係式が成立する。

$$\begin{aligned} \text{DetPol}(\tilde{M}_R) &= C \text{DetPol}(M_R), \quad \text{where} \\ C &= [\prod_{i=0}^q \text{lc}(H_{i,1}) \cdots \text{lc}(H_{i,r_i})] / [\text{lc}(H'_1) \cdots \text{lc}(H'_s)] \end{aligned} \quad (5.7)$$

命題 3 $F, G_1, \dots, G_q, r_0, r_1, \dots, r_q, C$ 等は上で定義されたものとする。 $r_0 + r_1 + \dots + r_q > s$ ならば、 $\tilde{F} \xrightarrow{\tilde{G}_1} \dots \xrightarrow{\tilde{G}_q} R$ の計算において、 $\text{lc}(H_{i,j})$, ($i=0, 1, \dots, q; j=1, \dots, r_i$), を独立なパラメータとみなすとき、 C を含まない全ての項は互いにキャンセルする。

証明 $r_0 + r_1 + \dots + r_q > s$ なので、 C の分母は分子を割り切ることを指摘しておく。 $R = \text{DetPol}(\tilde{M}_R)$ であり $\text{DetPol}(M_R)$ の各要素は $F_1, F_2, H'_1, \dots, H'_s$ の係数なので、命題は(5.7)から直ちに得られる。◇

第3章において、項キャンセルに対する命題1から桁落ちを規定する系1が得られた。同様に、命題2と3から【場合I】と【場合II】における桁落ちを規定する系が得られるが、紙面の制約のため記述を割愛する。

参 考 文 献

- [1] B. Buchberger. Gröbner Bases: An algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory*, N.K. Bose (Ed.), Chap. 6, Reidel Publ., 1985.
- [2] J.E. Collins. Subresultant and reduced polynomial remainder sequence. *J. ACM*, **14**, 128-142, 1967.
- [3] D. Cox, J. Little and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag New York, 1997.
- [4] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. *Proceedings of EUROCAL 1983; Springer-Verlag LNCS* **162**, 146-156, 1983.
- [5] R. Loos. Generalized polynomial remainder sequences. *Computer Algebra, Symbolic and Algebraic Computation*, B. Buchberger, G.E. Collins and R. Loos (Eds.), Springer-Verlag, 1983.
- [6] A.M. Mandache. The Gröbner basis algorithm and subresultant theory. *Proceedings of ISSAC'94 (Intn'l Symposium on Symbolic and Algebraic Computation)*, 123-128, ACM Press, 1994.
- [7] K. Nagasaka. A Study on Gröbner basis with inexact input. *Proceedings of CASC2009 (Computer Algebra in Scientific Computing): Springer LNCS* **5743**, 248-258, 2009.
- [8] T. Sasaki and A. Furukawa. Secondary polynomial remainder sequence and an extension of subresultant theory. *J. Inf. Proces.*, **7**, 175-184, 1984.
- [9] T. Sasaki and A. Furukawa. Theory of multiple polynomial remainder sequence. *Publ. RIMS (Research Inst. for Mathemat. Sci.)*, **20**, 367-399, 1984.
- [10] T. Sasaki and F. Kako. Computing floating-point Gröbner base stably. *Proceedings of SNC2007 (Symbolic Numeric Computation)*, 180-189, London, Canada, 2007.
- [11] T. Sasaki and F. Kako. Floating-point Gröbner basis computation with ill-conditionedness estimation. *Proceedings of ASCM2007 (Asian Symposium on Computer Mathematics): Springer LNAI* **5081**, 278-292, Deepak Kapur (Ed.), 2008.
- [12] T. Sasaki and F. Kako. Term cancellations in computing floating-point Gröbner bases. *Proceedings of CASC2010 (Computer Algebra in Scientific Computing): Springer LNCS* **6244**, to appear.